Policy Mapping Extension

References: X.509 sections: 3.3.17, 12.2.1, 12.2.2.7, 12.4.1
RFC 2459 sections: 4.2.1.6, 6.1
FPKI Profile sections: 1.2.7, 3.2.2.1, 3.2.2.1.1
MISPC sections: 3.1.3.1
DII PKI Functional Specification sections: 3.2.2.1.6

Implementation under analysis:

Analysis Date:

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Does the certificate issuer enable the policyMapping (PM) extension in CA certificates?		
Does the issuer not include the PM extension in EE certificates?		
Does the PM extension always have pairings of issuerDomainPolicy and subjectDomainPolicy in CA certificates?		
Does the issuer flag the extension as non-critical?		
Can the issuer include this extension in the self-signed certificates?		
Does the PM extension only have issuerDomainPolicy in self-signed certificates?		
Can cross-certificates be issued without a policy mapping extension?		1
In processing a received certificate with the PM extension present, does the certificate user recognize it as a CA certificate?		
Does the certificate user recognize that the listed issuer's certificate policies are considered equivalent to their paired subject's certificate policies?		

Other information:

Policy mapping: When a CA certifies a CA in another domain, a

Findings:

If the answer to all the analysis questions above is YES, then the implementation is compliant with the standards.

Recommendations for Standards Work: